REMARKS

The following remarks are responsive to the Office Action of May 13, 2009.

At the time of the Office Action, claims 1-30 were pending. Claims 1, 2 and 16 were now rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. ("A Method for Obtaining Digital Signatures and Public-Key Cryptosystems") in view of M'Raihi et al. (U.S. Patent No. 5,946,397). Claims 11 and 17 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al., and further in view of Gilbert et al. (U.S. Patent No. 5,987,138). Claims 12 and 18 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al., and further in view of Brickell (U.S. Patent No. 7,165,181). Claims 19 and 27 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al., and further in view of Kasahara et al. (U.S. Patent No. 6,788,788). Claims 20-22 and 28-30 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al. and Kasahara et al., and further in view of Arditti et al. (U.S. Patent No. 6,125,445). Claims 3 and 4 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al., and further in view of Arditti et al. Claims 5-7, 9-10 and 23-26 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al. and Arditti et al., and further in view of Kasahara et al. Claim 8 was rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of M'Raihi et al., Arditti et al. and Kasahara et al. and further in view of Gilbert et al. Claims 13-14 were rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of Kasahara et al. Claim 15 was rejected under 35 U.S.C. §103(a) as obvious over Rivest et al. in view of Kasahara et al., and further in view of Arditti et al. Claim 2 was also objected to.

In response to the objection, claim 2 is amended to correct a minor spelling error. Hence, Applicants respectfully request that this objection be withdrawn.

However, the rejections are respectfully traversed at least for the reasons set forth below.

Concerning the 35 U.S.C. §103(a) rejection of claims 1, 2 and 16 based on Rivest in view of M'Raihi, Applicants respectfully submit that Rivest fails to disclose the first step of generating, at the first entity, a first element of proof by using a generic number raised to a first power, modulo the modulus, having a first exponent equal to the public key exponent multiplied by a random integer, as recited in independent claim 1. Similar features are recited in independent claim 16 (and in independent claim 13 not included in this rejection).

In the Office Action, the Examiner contends that the first step of claim 1 of the present application is disclosed in Section V, line 16 through Section VI, line 22 of Rivest (which the Examiner refers to as "paragraph 5, line 16; paragraph 6, line 22"). However, Applicants respectfully submit that this passage of Rivest does not specify the details recited in the first step in claim 1 of the present application. Rather, Applicants understand that the Examiner considers this section of Rivest to disclose a first element of proof consisting in $M^{e.d}$.

However, Applicants again respectfully submit that Rivest does not disclose a first element of proof having a first exponent equal to the public key exponent multiplied by a random integer as explicitly recited in independent claims 1 and 16 (and also in independent claim 13 which is not included in this rejection). Rather, in Rivest, an element of proof C is generated on the basis of M^e, as is clearly described on page 122, right-hand column, 6th paragraph, of Rivest. Applicants submit that the exponent of the element of proof does not have a multiplication but consists only in a single positive integer e.

Applicants further respectfully submit that the only passage in Rivest where a multiplication e*d is mentioned on page 123, left-hand column, line 13. Applicants submit, however, that this multiplication only shows that the integer d, used for deciphering the encrypted message, can be derived from the integer e. Such a multiplication is not used in any kind of operation for generating a first element of proof.

Furthermore, Applicants submit that even assuming, simply for the purpose of argument, that the formula $M^{e.d}$ can be derived from Rivest, the integer d is not a random

integer, as explicitly recited in independent claims 1 and 16 (and independent 13). On the contrary, as is clear from the equation on page 123, left-hand column, line 13 of Rivest, the integer d is an integer derived from the other integer e (see also page 123, left-hand column, line 4 of Rivest).

In addition, Applicants respectfully submit that Rivest fails to disclose the second step of generating, at the first entity, a second element of proof related to the first element of proof and dependent on a common number shared by the first and second entities specifically for the transaction as recited in independent claim 1 (claims 13 and 16 also recite generating a second element of proof). The Examiner contends that the use of the public key in Rivest (i.e. the pair (e,n) according to the passage on page 122, right-hand column, 2nd paragraph) discloses this feature. In particular, the Examiner contends that the positive integer n would be the common number shared by the first and second entities on which the second element of proof depends.

However, Applicants respectfully submit that Rivest fails to disclose the generation of such a second element of proof at the first entity. Hence, even assuming, for purposes of argument only, that the public key (e,n) in Rivest is a second element of proof, Rivest does not disclose that the public key is generated at the first entity.

As indicated in the Office Action, The Examiner also acknowledges that Rivest does not disclose the third step of verifying, at the second entity, that the first element of proof is related through a relationship with a second power, modulo the modulus, of a generic number having a second exponent equal to a linear combination of at least part of the common number and of the public key exponent multiplied by the second element of proof, as recited in independent claim 1. Nevertheless, the Examiner contends that this feature is disclosed in M'Raihi, and therefore, one skilled in the art would have found it obvious to have modified Rivest in accordance with the teachings of M'Raihi to have achieved the embodiments of the present invention as recited in the rejected claims.

However, Applicants respectfully submit that M'Raihi does not teach the verifying relationship between $x=g^{ey+c}$. Rather, M'Raihi merely discloses that a signature element r is generated according to $r=g^{k}$, where k is a linear combination of xi values stored in a database (see col. 4, lines 15-43). M'Raihi fails to disclose that the linear combination uses at least a part of a common number, and the Office Action does not indicate which number in M'Raihi should be considered to be this common number.

Applicants further respectfully submit that M'Raihi fails to disclose that the linear combination uses a public key exponent. Applicants note that the only disclosure of a public key in M'Raihi is found in col. 3, line 46; where it is said that each entity has a public key y. However, such a public key y is not used in the computation of the exponent k.

Moreover, Applicants submit that M'Raihi fails to disclose that the linear combination uses a public key exponent multiplied by the second element of proof. Rather, the exponent k results from a linear combination of xi values, this is to say to a sum of ai*xi (see col. 4, line 35 of M'Raihi) where ai and xi are random numbers (col. 4, lines 9-10 and 28-30). These number being clearly stated as being random, they cannot be considered either as a public key exponent or as a second element of proof.

Accordingly, for at least these reasons, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to have modified the teachings of Rivest in accordance with the teachings of M'Raihi to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Accordingly, independent claims 1 and 16, and all of their dependent claims, should be allowable over these references.

Concerning the 35 U.S.C. §103(a) rejection of independent claim 13 and dependent claim 14 based on Rivest in view of Kasahara, Applicants respectfully submit that as discussed above, Rivest does not disclose a first element of proof having a first exponent equal to the public key exponent multiplied by a random integer as explicitly recited in independent claim 13. Applicants also submit that as discussed above, Rivest fails to disclose

generating a second element of proof related to the first element of proof and dependent on a common number specific for the transaction, as recited in independent claim 13.

Applicants further submit that Kasahara is being cited merely for its alleged teaching of a "communication means" as recited in independent claim 13. However, Applicants respectfully submit that Kasahara fails to make up for the deficiencies in the teachings of Rivest.

Hence, Applicants respectfully submit that one skilled in the art would not have found it obvious or possible to have modified the teachings of Rivest in accordance with the teachings of Kasahara to have achieved the embodiments of the present invention even as recited in independent claim 13. Accordingly, independent claim 13, and all of its dependent claims, should be allowable over these references.

Concerning the rejections of the dependent claims based on Rivest in various combinations with M'Raihi, Gilbert, Brickell, Kasahara and Arditti, Applicants submit that M'Raihi and Kasahara are being cited for the reasons discussed above and, as with Gilbert, Brickell and Arditti, are further being cited as allegedly teaching the specific features of the dependent claims against which they are applied. Applicants submit, however, that these references fail to make up for the deficiencies in the teachings of Rivest as discussed above. Hence, one skilled in the art would not have found it obvious or possible to have modified Rivest in accordance with the teachings of these references to have achieved the embodiments of the present invention even as recited in independent claims 1, 13 and 16. Thus, all claims should be allowable.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Joseph J. Buczynski, Reg. No. 35,084
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: August 12, 2009

CH01/ 25364869.2